



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/697,397	10/29/2003	Laurence Lundblade	030457	7478

23696 7590 09/21/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER

LASHLEY, LAUREL L

ART UNIT	PAPER NUMBER
----------	--------------

2132

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

09/21/2007

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kscanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/697,397	LUNDBLADE, LAURENCE	
	Examiner	Art Unit	
	Laurel Lashley	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07/3/07.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendments filed 07/03/07 with regard to claims 1-45 have been accepted and entered. The amendments however have introduced new claim rejections.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 1- 45 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for an application identifier, does not reasonably provide enablement for a non-arbitrary application identifier. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to use the invention commensurate in scope with these claims. The portion of paragraph [0048] (lines 4-5), which the Applicant has cited as support for the amendment claiming a non-arbitrary application ID, states that a application ID is checked, then provided so that an application cannot guess an ID randomly resulting in unauthorized access to credentials. Furthermore, since paragraph [0049] by example offers a hash function as a means by which to generate an application credential, the specification supports an arbitrary ID.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1 – 45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2132

4. Claims 2- 5, 7 -12, 14-16, 19-22, 25-27, 29-30, 33-34, 37- 38, and 40-45 recites the limitation "the application identifier". There is insufficient antecedent basis for this limitation in the claim.
5. Claims 7 -12, 14-16, 19-22, 25-27, 29-30, 33-34, 37- 38, and 40-45 recites the limitation "the non-arbitrary application credential". There is insufficient antecedent basis for this limitation in the claim.
6. Claims 1 - 45 are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. Evidence that claims 1-45, particularly independent claims 1, 7, 13, 18, 24, 28, 32, 36 and 40 fail to correspond in scope with that which applicant(s) regard as the invention can be found in the reply filed 07/03/07. In that paper (see REMARKS, page 10), applicant has stated "[h]ash functions, by their operation, produce arbitrary results. Thus, by using a hash function, Drews specifically teaches the use of an arbitrary ID." and as such fails to teach having a non-arbitrary application ID, and this statement indicates that the invention is different from what is defined in the specification because paragraphs [0032] and [0049] of the instant application teaches the generation of an application credential using a hash function.

Response to Arguments

7. Applicant's arguments filed 07/03/07 have been fully considered but they are not persuasive. It is Applicant's assertion that none of the cited art teaches or suggests the use of a non-arbitrary application identifier. Applicant's argument is considered moot in view of the abovementioned rejections.

It is Applicant's contention the cited art also does not suggest the combination of any application ID and the master credential. The Examiner respectfully disagrees.

Art Unit: 2132

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Drews discloses ensuring the authority and integrity of information used to verify credentials. Bari et al. discloses managing authentication credentials that allow users access to services and devices. As such the motivation for modifying Drews to incorporate the combination of the application ID and master credential as in Bari et al. is to ensure authorized user/device authentication.

It is also Applicant's assertion that "[e]ven though Drews discloses both the application ID and the public key (master credential), Drews never suggests combining the two to create an application credential. If this was obvious to one of skill in the art, it should be disclosed in Drews. "

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

For at least these reasons, the Examiner maintains the rejection of claims 1-45.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject

Art Unit: 2132

matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1-45 are rejected under 35 U.S.C. 103(a) as being obvious over Drews, U.S.

Patent No. 6,477,645 B1, (hereinafter "Drews") in view of Bari et al., U.S. Patent Publication No. 2002/0023059 A1, (hereinafter "Bari").

9. Regarding **claim 1**: Drews discloses a method (col. 6 lines 15-16) for providing an application credential to an application running on a device (col. 2 lines 9-12), wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the method comprising:

receiving a request to generate the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for application credential), a variable length amount of digital data (application identifier)); and

generating the application credential using the application identifier (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

10. Regarding **claim 7**: Drews discloses an apparatus (col. 2 lines 9-22) that operates to provide an application credential to an application running on a device (col. 2 lines 9-12), wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the apparatus comprising:

receiving logic that operates to receive a request for the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (receiving logic) input (request for application credential), a variable length amount of digital data (application identifier)); and

generating logic that operates to generate the application credential using the application identifier (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating logic)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to combine the teachings of Drews with the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

11. Regarding **claim 13**: Drews discloses an apparatus (col. 2 lines 9-22) that operates to provide an application credential to an application running on a device (col. 2 lines 9-12), wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the apparatus comprising:

Art Unit: 2132

means for receiving a request for the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (means for receiving) input (request for application credential), a variable length amount of digital data (application identifier)); and

means for generating the application credential using the application identifier and a master credential (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (means for generating).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

12. Regarding **claim 18**: Drews discloses a computer-readable media (col. 7 line 2) comprising instructions, which when executed by a processor in a device, provide an application credential to an application running on a device (col. 2 lines 9-12), wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the computer readable media comprising:

instructions for receiving a request for the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for application credential), a variable length amount of digital data (application identifier)); and

Art Unit: 2132

instructions for generating the application credential using the application identifier and a master credential means for generating the application credential using the application identifier and a master credential (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

13. Regarding **claim 24**: Drews discloses a method for operating a credential server (col. 6 lines 15-16) to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the method comprising:

receiving an non-arbitrary application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for server credential), a variable length amount of digital data (application identifier));

generating the server credential using the non-arbitrary application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential

Art Unit: 2132

server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating)); and transmitting the server credential to the data server (col. 2 lines 9-32), wherein if the server credential and the application credential match, the application is authenticated (col. 4 lines 9-36, authorizing entity supplies (transmits) transformation value (server credential) to user/agent that submits (transmits) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

14. Regarding **claim 28**: Drews discloses an apparatus (col. 2 lines 9-22) for use with a credential server to authenticate an application running on a device, wherein the application transmits a request for data to a data server (col. 2 lines 34-42) and the request comprises an application credential (col. 3 line 24), the apparatus comprising:

first receiving logic that operates to receive an non-arbitrary application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity, generates and supplies (upon request) transformation values

Art Unit: 2132

(server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receiving logic) input (request for server credential), a variable length amount of digital data (application identifier));

generating logic that operates to generate the server credential based on the non-arbitrary application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating logic)); and

transmitting logic that operates to transmit the server credential to the data server (col. 2 lines 9-32), wherein the data server matches the server credential to the application credential to authenticate the application (col. 4 lines 9-36, authorizing entity supplies (transmitting logic) transformation value (server credential) to user/agent that submits (transmitting logic) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

Art Unit: 2132

15. Regarding **claim 32**: Drews discloses an apparatus (col. 2 lines 9-22) for use with a credential server to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the apparatus comprising:

means for receiving an non-arbitrary application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (means for receiving) input (request for server credential), a variable length amount of digital data (application identifier));

means for generating the server credential based on the non-arbitrary application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (means for generating)); and

means for transmitting the server credential to the data server (col. 2 lines 9-32), wherein the data server matches the server credential to the application credential to authenticate the application (col. 4 lines 9-36, authorizing entity supplies (means for transmitting) transformation value (server credential) to user/agent that submits (means for transmitting) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value

Art Unit: 2132

(server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

16. Regarding **claim 36**: Drews discloses a computer-readable media (col. 7 line 2) comprising instructions, which when executed by a processor in a credential server, operate to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the computer-readable media comprising:

instructions for receiving the application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for server credential), a variable length amount of digital data (application identifier));

instructions for generating the server credential based on the non-arbitrary application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col.

Art Unit: 2132

3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating)); and

instructions for transmitting the server credential to the data server (col. 2 lines 9-32), wherein the data server matches the server credential to the application credential to authenticate the application (col. 4 lines 9-36, authorizing entity supplies (transmits) transformation value (server credential) to user/agent that submits (transmits) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

17. Regarding **claim 40**: Drews discloses a method (col. 6 lines 15-16) for processing an application credential associated with an application running on a device, wherein the application credential is used by the application to authenticate to a data server, the method comprising:

receiving a request to generate the application credential, wherein the request includes an non-arbitrary application identifier (col. 3 line 15-19, transformation value generator, hash

Art Unit: 2132

function, accepts (receives) input (request for application credential), a variable length amount of digital data (application identifier)); and

generating the application credential using the non-arbitrary application identifier (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating).

transmitting a request for data to a data server (col. 2 lines 9-22), wherein the request comprises the application credential (col. 6 lines 15-44, authorizing entity identifies newly installed workstation requiring installation of a boot image (request for data), and transformation value (application credential) is necessary to obtain data).

(col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator

requesting a server credential from a credential server, wherein the request for the server credential comprises the application identifier (col. 3 line 16) and a token (col. 2 line 44) by which the data server authenticates itself (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for server credential), a variable length amount of digital data (application identifier));

generating the server credential using the non-arbitrary application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials)

Art Unit: 2132

performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating)); and transmitting the server credential to the data server (col. 2 lines 9-32),

matching the server credential with the application credential, wherein the application is authenticated if the two credentials match (col. 4 lines 9-36, authorizing entity supplies (transmits) transformation value (server credential) to user/agent that submits (transmits) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)); and transmitting the data to the application (col. 6 lines 22-32).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (see Bari, ([0036] lines 2-5)).

18. Regarding **claims 2, 8, 14, 22, and 41**: Drews discloses a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the application credential (col. 3 lines 15-33).

19. Regarding **claims 3, 9, 15, 19, and (42)**: Drews discloses using a modification detection and authentication technique (col. 3 lines 49-65) to determine if the application or the application

Art Unit: 2132

identifier has been modified (col. 3 lines 24-40) and prove the application is associated with the application identifier (col. 3 lines 24-40).

20. Regarding **claims 4, 10, 16, and 20**: Drews discloses the modification detection and authentication technique (col. 3 lines 49-65) is generated by a server that is distinct from a provider of the application (col. 3 lines 54-56).

21. Regarding **claims 5, 11, 17, 21, and 43**: Drews discloses the modification detection and authentication technique is a digital signature (col. 2 lines 42-52).

22. Regarding **claims 6, 12, 23, and 45**: Drews discloses the device is a wireless device (col. 2 lines 53-65).

23. Regarding **claims 25, 29, 33, 37, and 44**: Drews discloses receiving an authentication token (col. 2 line 44) that proves the request is associated with the application identifier (col. 2 lines 42-52).

24. Regarding **claims 26, 31, 35, and 39**: Drews discloses receiving the application credential (col. 3 lines 34-40); matching the application credential and the server credential (col. 3 lines 34-40); and transmitting an authorization to the data server to fulfill the data request if the application credential matches the server credential (col. 6 lines 15-54).

Art Unit: 2132

25. Regarding **claims 27, 30, 34, and 38**: Drews discloses generating the server credential (col. 3 lines 63-65) using a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the server credential (col. 3 lines 15-33).

Conclusion

26. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

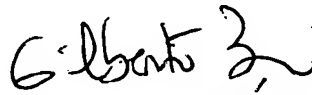
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132



LLL

06 September 07



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100